DMP:ICR/SKW/EHS
F:2022R00326

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH THE FOLLOWING ACOUNTS: PROFITOFDOOM8888@GMAIL.COM; PROPHETOFTRUTH88@GMAIL.COM; AND THAT ARE STORED AT PREMISES CONTROLLED BY GOOGLE LLC; FRANKJAMES20048@MSN.COM THAT IS STORED AT PREMISES CONTROLLED BY MICROSOFT CORP.; FRANKJAMES20048@AOL.COM THAT IS STORED AT PREMISES CONTROLLED BY YAHOO, INC.; FRANKJAMES1326@MAIL.COM THAT IS STORED AT PREMISES CONTROLLED BY 1&1 INC.; FACEBOOK USER ID 10000258632238; THAT IS STORED AT PREMISES CONTROLLED BY META PLATFORMS, INC.; AND APPLE ID FRANKJAMES20048@MSN.COM THAT IS STORED AT PREMISES CONTROLLED BY APPLE INC.	Case No. 22-MJ-1170

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Ian Franckling, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the following accounts which collectively are referred to as the Subject Accounts:

Google LLC

Account	User
profitofdoom8888@gmail.com	FRANK JAMES
Prophetoftruth88@gmail.com	FRANK JAMES

(the "Google Accounts") that are stored at premises controlled by Google LLC ("Google"), an electronic communication and remote computing service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043;

Microsoft Corp. (MSN)

Account	User
frankjames20048@msn.com	FRANK JAMES

(the "Microsoft Account") that is stored at premises controlled by Microsoft Corp. ("Microsoft"), an electronic communication and remote computing service provider headquartered at One Microsoft Way, Redmond, Washington;

Yahoo Inc. (AOL)

Account	User
frankjames20048@aol.com	FRANK JAMES

(the "AOL Account") that is stored at premises controlled by Yahoo Inc. (formerly known as Oath Holdings Inc. and AOL) ("AOL"), an electronic communication and remote computing service provider that accepts service of legal process at 1199 Coleman Avenue, San Jose, CA 95110;

1&1 (mail.com)

Account	User
frankjames1326@mail.com	FRANK JAMES

(the "Mail.com Account") that is stored at premises controlled by 1&1 IONOS Inc. ("Mail.com"), an electronic communication and remote computing service provider that accepts service of legal process at 701 Lee Road, Suite 300, Chesterbrook, PA 19087;

Meta, Inc. (Facebook)

Account Number	Display Name	User
10000258632238	Frank Whitaker	FRANK JAMES

(the "Facebook Account") that is stored at premises owned, maintained, controlled, or operated by Meta Platforms Inc. ("Meta"), an electronic communication and remote computing service provider headquartered at 1601 Willow Road in Menlo Park, California; and

Apple Inc.

Account	User
frankjames20048@msn.com	FRANK JAMES

(the "Apple Account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California.

2. The information to be searched is described in the following paragraphs and in Attachments A1, A1, A3, A4, A5, and A6. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A), and 2703(c)(1)(A) to require the providers of the Subject Accounts to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachments B1, B2, B3, B4, B5, and B6. Upon receipt of the information described in Section I of Attachments B1,

B2, B3, B4, B5, and B6, government-authorized persons will review that information to locate the items described in Section II of Attachments B1, B2, B3, B4, B5, and B6.

3. I am a Special Agent with the Federal Bureau of Investigation ("FBI"). I have been a Special Agent with the FBI since 2021. As an FBI Special Agent, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. During my tenure working at the FBI, I have participated in investigations of violent criminals and have used a variety of investigative techniques, including, but not limited to, interviews of witnesses, cooperating witnesses, and confidential informants; physical surveillance; reviews of telephone records; and search warrants as to physical premises and electronic devices and cloud services.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrants and does not set forth all of my knowledge about this matter.

5. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1992(a)(7), (a)(10), (b)(1), (c)(1), and (c)(2) (terrorist attacks or other violence against mass transportation systems) and 18 U.S.C. § 924(c)(1)(A)(i), (c)(1)(A)(ii), and (c)(1)(A)(iii) (use of a firearm during a crime of violence) (the "Subject Offenses") have been committed by FRANK JAMES. There is also probable cause to search the information described in Attachments A1, A2, A3, A4, A5, and A6, for evidence and instrumentalities of the Subject Offenses and criminal conduct described herein.

JURISDICTION

6. This Court has jurisdiction to issue the requested warrants because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

A. Offense Conduct

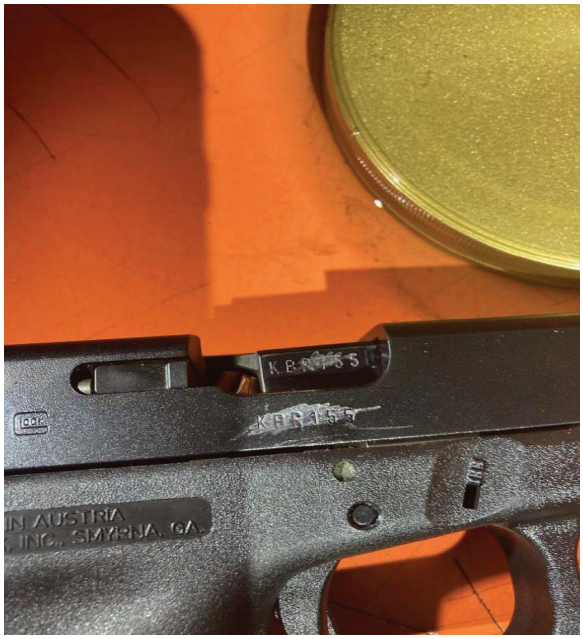
7. At approximately 8:26 a.m. on April 12, 2022, a shooting incident occurred aboard a subway train located at 36th Street in Brooklyn, New York.

8. Videos posted shortly afterward to open-source channels such as Twitter appeared to depict the scene. The videos showed a stopped subway train that was pouring smoke out its doors. The videos also showed one or more subway passengers who were lying prone on the floor of the station, just outside the train. Multiple victims were taken to the hospital with gunshot wounds and for smoke inhalation.

9. Law enforcement officers who interviewed passengers were told that the perpetrator set off one or more smoke-emitting devices in the train car, wore a gas mask or similar protective device, and appeared to be carrying a large number of items. Some passengers also told the law enforcement officers that the perpetrator fired a gun multiple times at passengers in the train car. Some passengers also told law enforcement officers that the assailant was dressed in what appeared to be a construction worker's vest.

10. Searches of the scene of the attack revealed a firearm. The firearm was a Glock 17 pistol manufactured in Austria. Records provided by the Bureau of Alcohol, Tobacco, Firearms and Explosives revealed that the firearm was lawfully purchased in Ohio by an

individual named "Frank Robert James." Marks on the serial number on the firearm appear to reflect that an attempt was made to deface the serial number, as reflected in the photo below:



11. Subsequent ballistic analysis confirmed that shell casings found on the subway car matched the pin impression from the Glock 17 pistol, indicating the Glock 17 pistol fired the bullets on the subway car.

12. Also found at the scene of the attack was a torch, a Samsung cellular phone (the "James Samsung Phone"), a U-Haul key, an orange reflective jacket, a KwikSaftey yellow hard hat, a Baofeng radio, fireworks from a firework company ("Fireworks Company 1"), Enola EG18X smoke grenades, 9 mm Luger +P 90 Grain ammunition, an East Sport backpack, and multiple bank cards including a bank card issued by a United States financial institution ("Bank-1") in the name of "Frank James." Records provided by Bank-1 indicated multiple telephone numbers associated with the account, including a telephone number with Milwaukee, Wisconsin area code 414, ending in 2903 (the "2903 Number").

13. Records provided by U-Haul revealed that, on or about April 11, 2022, at approximately 2:03 p.m., an individual named "Frank James" rented from U-Haul in Philadelphia, Pennsylvania, a white Chevrolet Express Model G2500 Cargo Van with Arizona plates (the "U-Haul Vehicle"). U-Haul records reflected that the individual reserved and pre-paid for the rental on or about April 6, 2022, provided U-Haul with the 2903 Number as his contact information, and advised U-Haul that he preferred to be contacted by text message at that number. That individual also provided U-Haul with a Wisconsin driver's license in the name of "Frank Robert James," with an address in Milwaukee, Wisconsin, and a date of birth in 1959.

14. New York City Police Department video surveillance cameras recorded the U-Haul Vehicle driving over the Verrazano Narrows Bridge at approximately 4:11 a.m. on April 12, 2022, and entering Brooklyn, New York. The U-Haul Vehicle crossed state lines from Pennsylvania to New Jersey and then to New York. A photograph of the U-Haul Vehicle driving over the Verrazano Narrows Bridge is below:

15. At approximately 6:12 a.m. on April 12, 2022, a surveillance camera located at West 7th Street and Kings Highway in Brooklyn, New York, recorded an individual wearing a yellow hard hat, orange working jacket with reflective tape, carrying a backpack in his right hand and dragging a rolling cart in his left hand, leaving the U-Haul Vehicle on foot. A photograph from the surveillance video is below:

16. Law enforcement subsequently located the U-Haul Vehicle parked on the side of the road in the vicinity of 366 Kings Highway in Brooklyn, New York. Notably, the location is approximately two blocks from a New York City Transit N-train subway stop.

17. Law enforcement officers spoke to an individual, whose identity is known to the affiant, who was on the subway during the April 12, 2022 attack. The individual identified the attacker as a heavy-set man wearing an orange reflective jacket, yellow hard hat and paper face mask, and carrying a large roller bag. Law enforcement officers then showed the surveillance video from West 7th Street and Kings Highway described above. The individual stated, in sum and substance, that the physical build, orange jacket and yellow hard hat of the individual depicted on the video matched that of the attacker. In addition, the individual stated, in sum and

substance, that the roller bag in the video matched the roller bag that he saw the attacker holding on the subway.

18. As noted above, the attack took place at approximately 8:26 a.m. on April 12, 2022. At approximately 8:40 a.m., a surveillance camera recorded an individual who appears to match FRANK JAMES's photographs from law enforcement databases and the Wisconsin Department of Motor Vehicle records, walking up the stairs and exiting the New York City Transit N-train subway stop located at 25th Street, one subway stop away from the approximate location of the attack at the 36th Street subway station. A still image from the surveillance video is included below.

19. Additionally, law enforcement agents recovered from the scene a receipt for storage unit #0318 with a particular storage facility. Information provided by the storage facility indicated that the unit, which was located in Philadelphia, Pennsylvania was registered to

FRANK JAMES. Records from Lyft revealed that JAMES visited the storage facility at approximately 6:17 p.m. on April 11, 2022, the day before the attack.

20. On April 12, 2022, law enforcement agents executed a court-authorized warrant to search the storage unit registered to FRANK JAMES. Inside, law enforcement agents recovered, among other items, 9mm ammunition, a threaded 9mm pistol barrel that allows for a silencer or suppresser to be attached, target, .223 caliber ammunition, which is used with an AR-15 semi-automatic rifle, an Alcatel cellular phone (the "James Alcatel Phone"), and an LG cellular phone (the "James LG Phone").

21. Law enforcement also identified an apartment used by FRANK JAMES in Philadelphia, Pennsylvania. Records from Lyft revealed that an account associated with JAMES ordered Lyft rides to or from the Philadelphia apartment approximately 21 times from March 28, 2022 through April 10, 2022. Information provided by the management company revealed that JAMES rented the apartment for approximately 15 days beginning on or about March 28, 2022.

22. On April 13, 2022, law enforcement agents executed a court-authorized warrant to search the Philadelphia apartment rented by FRANK JAMES. Inside the apartment, law enforcement agents recovered, among other items, an empty magazine for a Glock handgun, a taser, a high-capacity rifle magazine and a blue smoke cannister.

B. The Defendant's Arrest

23. On or about April 13, 2022, the Honorable Roanne L. Mann, United States Magistrate Judge, Eastern District of New York, signed a complaint and warrant authorizing FRANK JAMES's arrest on a complaint charging him with violating 18 U.S.C. § 1992(a)(7) and (b)(1). See Docket No. 22-MJ-429 (RLM) at 1.

24. On or about April 13, 2022, FRANK JAMES (or the "defendant") was arrested. He was in possession of an iPhone (the "James iPhone") at the time of his arrest.

25. On or about April 14, 2022, FRANK JAMES was arraigned on the complaint and ordered detained at the Metropolitan Detention Center (the "MDC") in Brooklyn, New York.

26. On or about May 6, 2022, a grand jury sitting in the Eastern District of New York returned an indictment charging FRANK JAMES with violating 18 U.S.C. § 1992(a)(7), (a)(10), (b)(1), (c)(1), and (c)(2), as well 18 U.S.C. § 924(c)(1)(A)(i), (c)(1)(A)(ii), and (c)(1)(A)(iii). See Docket No. 22-CR-214 (WFK) at 15.

C. Evidence that the Defendant Planned the April 2022 Attack

27. Subsequent investigation revealed that FRANK JAMES began preparing for the April 12, 2022 attack years earlier.

28. For example, according to PayPal payment records, on or about January 8, 2017 and June 29, 2019, FRANK JAMES purchased Enola Gaye EG18X smoke grenades using his PayPal account. The same brand of smoke grenades was recovered from the scene of the attack.

29. According to records from a firearms supply company ("Firearms Supply Company-1"), on or about October 23, 2019, FRANK JAMES purchased multiple boxes of Underwood Xtreme Defender 9mm Luger +90 Grain ammunition which were shipped to a "Frank James" in Milwaukee, Wisconsin. The same brand of ammunition was used to shoot multiple victims during the April 12, 2022 attack and was recovered from the scene of the attack.

30. According to records from Amazon, on or about May 14, 2021, FRANK JAMES purchased an East Sport backpack using his Amazon account. The same brand of backpack was recovered from the scene of the attack. In addition, on or about May 17, 2021, FRANK JAMES purchased a KwikSaftey yellow hard hat using his Amazon account. Notably, on or about April

12, 2022, JAMES was captured on video wearing a yellow hard hat before entering the Kings Highway N train subway station in Brooklyn. A KwikSaftey yellow hard hat was also recovered from the scene of the attack.

31. According to records from Fireworks Company 1, on or about June 21, 2021, FRANK JAMES purchased various fireworks including "color smoke balls," "smoke bombs", and a "safety fuse." Fireworks matching the items that JAMES purchased in 2021 from Fireworks Company 1 were recovered from the scene of the attack.

32. Electronic evidence further shows that FRANK JAMES planned the April 12, 2022 attack, including by Googling terms related to the attack.

33. For example, pursuant to a search warrant signed on or about April 12, 2022 by the Honorable Ramon E. Reyes, Jr., law enforcement officers searched the James Samsung Phone which was recovered from the scene of the attack. See 22-MJ-421 (RER). Based on records from Tracfone, which registered the telephone number of the James Samsung Phone, the subscriber's date of birth was listed as JAMES's date of birth and the subscriber name was left blank. In addition, a search of the James Samsung Phone revealed information connecting the phone to JAMES, including approximately five saved photographs of JAMES dated approximately April 2022. JAMES's Lyft account, which was registered using the name "Frank James" and the email address frankjames2048@aol.com, was also connected to the James Samsung Phone.

34. The search of the James Samsung Phone also revealed that the device was used to conduct electronic searches in preparation for FRANK JAMES's April 12, 2022 attack.

a. On or about March 19, 2022, the user of the James Samsung Phone conducted Google searches for the phrases "gun shops near Columbus Ohio" and "can I buy a gun in Ohio if I'm not a resident."

b. On or about March 20, 2022, the user of the James Samsung Phone searched for the address of the Philadelphia apartment that the defendant resided in during the week before the attack.

c. On or about March 21, 2022, the user of the James Samsung Phone searched for the name of the storage facility that that the defendant visited the day before the attack, the receipt of which was found at the scene of the attack.

d. On or on about April 1, 2022, the user of the James Samsung Phone searched for "MTA," "New York," "transit," "stops on the N train."

e. On or about April 6, 2022, the user of the James Samsung Phone searched for "311 kings highway brooklyn ny," which is near where JAMES parked the U-Haul van before entering the N street subway station on April 12, 2022.

35. An audio file was also saved on the James Samsung Phone which appears to be a recording of FRANK JAMES discussing an imminent attack. In the audio recording, JAMES stated in sum and substance that he was making the recording on January 2, 2022.[1] Speaking to his listeners about his death, the defendant made the following statements:

[1] Although in the audio file the defendant states that the file was recorded on January 2, 2022, the date of the audio file saved on the James Samsung Phone is April 3, 2022, the same month as the attack.

a. "You're going to know for a fact that I'm gone, they'll be no question about that . . . when I go out of this motherfucker . . . everyone's gonna know it was me;"[2]

b. "If you hear the name Frank James on the news, if something happens to a Frank James that's sixty-something years old, chances are that's me."

c. "Download my videos while you can because they're probably going to delete my channel."

36. Pursuant to a search warrant signed by the Honorable Judge Mann on or about April 12, 2022, law enforcement officers also searched the James Alcatel Phone and the James LG Phone which were recovered from storage unit number 0318, the Philadelphia storage unit that the defendant rented and visited before the attack. A search of the James Alcatel Phone revealed information connecting FRANK JAMES to the phone, including that the device was connected to JAMES's accounts, including his email account frankjames20048@msn.com. In addition, there were electronic copies of JAMES's resume, birth certificate, and driver's license saved on the phone.

37. A search of the James Alcatel Phone also revealed evidence that FRANK JAMES planned and carried out the attack. For example, a search of the James Alcatel Phone uncovered images saved on or about May 3, 2019, May 21, 2019, September 25, 2019, and September 26, 2019 of 9mm Luger +P 90 Grain ammunition, the same ammunition used in the attack and the same ammunition JAMES purchased on or about October 23, 2019. The James Alcatel Phone also had a saved image dated on or about August 20, 2019 of a Baofeng radio, the same brand of radio which was recovered from the scene of the attack as well as a saved photograph dated on or

[2] All quotations from videos and social media include original grammar.

about December 6, 2019 of a man wearing what appears to be a Baofeng radio. The man's face is blocked in the photograph.

38. In addition, saved on the James LG Phone are undated images of a yellow hard hat, an orange reflective jacket, and an East Sport package, similar to the items found at the scene of the attack.

39. Pursuant to a search warrant signed on or about April 13, 2022 by the Honorable Judge Mann, law enforcement officers also searched the James iPhone, which was recovered from FRANK JAMES at the time of his arrest. See 22-MJ-432 (RLM). A search of the James iPhone revealed Google searches of the terms "crime stop" and "crime stoppers." The call log showed a call to NYPD CrimeStoppers on or about April 13, 2022, the date JAMES called police to report his whereabouts after committing the attack.

D. The Defendant Discusses Violent Acts in Social Media Posts

40. FRANK JAMES also discussed his desire to commit mass violence and potential motivations and plans for the subway shooting in social media posts across various platforms and accounts before the April 12, 2022 attack.

41. On YouTube (which is owned by Google LLC), FRANK JAMES used his Google Accounts to post videos under multiple display names connected to his Google Accounts, including the display names "profitof_doom8888" and "prophet_oftruth88." I assess that the individual in videos posted by the display names connected to the Google Accounts is JAMES. According to subscriber information from Google, the Google Account profitofdoom8888@gmail.com is connected to the display name profitof_doom8888. The subscriber name on the Google Account profitofdoom8888@gmail.com is "profitofdoom8888" and the recovery email address is frankjames20048@aol.com, the AOL Account. In addition,

the subscriber telephone number is the 2903 Number, which is the telephone number associated with JAMES. The billing information is listed as "Frank James" with the email address frankjames20048@msn.com, the Microsoft Account. According to subscriber information from Google, the Google Account prophetoftruth88@gmail.com is connected to the display name prophet_oftruth88. The subscriber of the Google Account prophetoftruth88@gmail.com is listed as "prophetoftruth88" and the recovery email address is frankjames20048@aol.com, the AOL Account. In addition, the subscriber telephone number is the 2903 Number. The billing information is in the name of "Frank James" with a billing email address of frankjames20048@msn.com, the Microsoft Account. In addition, the Google Account prophetoftruth88@gmail.com is connected to the email feature on the James Samsung Phone, which was recovered from the subway platform on or about April 12, 2022. Based on a review of the James Samsung Phone, JAMES received multiple emails from YouTube to prophetoftruth88@gmail.com regarding the videos he posted on YouTube, including an email dated April 4, 2022 informing JAMES that someone commented on a video he posted using the display name prophet_oftruth88 title "Sensible Violence."

42. In multiple videos posted on YouTube using the display name "profitof_doom8888" (which is connected to the Google Account profitofdoom8888@gmail.com), FRANK JAMES made statements about trips to New York, the need for people to die, and foreshowed his future subway attack.[3]

[3] The videos described herein were downloaded from YouTube by law enforcement agents immediately after the defendant's April 12, 2022 attack.

43. For example, in a video posted in 2019 discussing traveling to New York, FRANK JAMES stated "at the very least it's going to be very interesting. Let me say that. It's going to be very interesting what happens in New York with me." In another video, the date of which is unknown at his time, JAMES repeatedly referenced "dying time" and stated that the dying time "has to happen for the possibility for change." In a third video, JAMES stated that the "whole system is coming down" just like the World Trade Center after the September 11, 2001 terrorist attack. In other videos, JAMES stated how people are "better off dead" and repeatedly discussed how the human population has to be reduced to survive. JAMES also made statements indicating that he had "nothing to lose" due to his age.

44. FRANK JAMES used the display name "prophet_oftruth88" (which is connected to the Google Account to prophetoftruth88@gmail.com) to post similar videos. For example, in a YouTube video posted before the April 12, 2022 attack, JAMES made various statements about the New York City subway system and an upcoming trip to New York. Among other things, JAMES addressed statements to New York City's mayor: "What are you doing, brother? What's happening with this homeless situation?" and "Every car I went to wa[s] loaded with homeless people. It was so bad, I couldn't even stand." JAMES further called for the end of humanity and stated that he was full of hate, anger, and bitterness.

45. In another video posted using the display name "prophet_oftruth88" FRANK JAMES foreshadowed his future attack, stating: "the shit that I'm thinking about, I have a lot of moving parts to do my shit, so I have to make sure they're set to go, so I have to make sure they don't fizzle out or they don't miss deploy or some shit." JAMES went on to state that "if you keep fucking with me, one or both of us is not going to be on this earth anymore, which is going to be a good thing because there's too many beings on this healthy anyway." In another

video, JAMES stated that a "factory reset should take place" and instructed his followers to "get a gun" and that you "can't kill every motherfucker but you can get two or three before they get you and yours." In a different video, JAMES stated that Ted Bundy is one of his heroes and that he wants to "be like those motherfuckers that got away with that shit."

46. According to open-source information, FRANK JAMES frequently posted his own YouTube videos from his Google Accounts to his Facebook Account, using the display name "Frank Whitaker" and a display image of a photograph of JAMES. In addition to reposting his YouTube videos, JAMES posted other messages on his Facebook Account as well. For example, on or about April 8, 2022, JAMES posted an image of a man, not JAMES, pointing the barrel of a gun directly at the camera. On or about March 3, 2022, JAMES posted a YouTube video titled "YOUTUBE.COM AND NOW I BECOME DEATH." On or about February 19, 2022, JAMES posted an image of what appear to be deceased feet in a morgue with the tag "D.O.A," which I am aware stands for "dead on arrival."

E. The Accounts To Be Searched

47. There is probable cause that the Subject Accounts will contain evidence and instrumentalities of the Subject Offenses, including, among other evidence, evidence of FRANK JAMES's motive in committing the April 12, 2022 attack, JAMES's identity as the attacker, and JAMES's preparation and planning for the attack.

i. The Google Accounts

48. There is probable cause to search the Google Accounts. As discussed above, FRANK JAMES used both Google Accounts to post videos on YouTube related to his plans to travel to New York, his plans to carry out an attack; and his motivate for an attack. According to records from Google, the Google Account profitofdoom8888@gmail.com was created on or

about July 1, 2018 and last updated on or about March 8, 2022, approximately one month before the attack. The Google Account Prophetoftruth88@gmail.com was created on or about May 7, 2014 and last used on or about April 11, 2022 and April 12, 2022, the day before and the day of the attack. According to Google records, location data is associated with the Google Accounts.

49. Accordingly, there is probably cause that the Google Accounts will contain evidence of the Subject Offenses, including JAMES's motive, his planning of the attack, his location when planning and carrying out the attack, and his identity as the individual posting the YouTube videos and carrying out the attack.

ii. The Microsoft Account

50. There is probable cause the search the Microsoft Account. Records from Microsoft indicate that the subscriber's name is "Frank James" and the billing email address is frankjamse1326@mail.com.[4] In addition, the Microsoft Account was logged into the James Samsung Phone—the phone found at the scene of the attack—and is one of the email addresses associated with FRANK JAMES's Lyft account. The Microsoft Account was also the email address associated with JAMES's bank account at Bank-1. Furthermore, the email address associated with the Microsoft Account is in JAMES's true name: frankjames20048@msn.com.

51. In addition, the Microsoft Account is the email address associated with various e-commerce websites that FRANK JAMES used to purchase items used in his attack. For example, the Microsoft Account was the email account associated with JAMES's PayPal account

[4] Records from Microsoft indicate that the account may have been deleted. This search warrant will confirm whether or not Microsoft has retained any data for the Microsoft Account.

which he used to purchase smoke grenades on or about January 8, 2017 and June 29, 2019. The Microsoft Account was also the email account associated with JAMES's Amazon account which he used to purchase an East Sport backpack on or about May 14, 2021 and a KwikSaftey hard hat on or about May 17, 2021. Based on my training and experience, I know that e-commerce websites typically send e-mail confirmations to the associated email account. Accordingly, there is probable cause that the Microsoft Account will contain evidence of the Subject Offenses, including JAMES's planning of the attack and his identity as the individual carrying out the attack.

iii. The AOL Account

52. There is probable cause the search the AOL Account. According to records from AOL, the subscriber of the AOL Account is "Robert James" with a recovery email address of frankjames20048@msn.com, the Microsoft Account, and recovery phone the 2903 Number. Based on my investigation to date, I am aware that "Robert" is FRANK JAMES's middle name. The subscriber telephone number is the 2903 Number. In addition, the AOL Account was created on September 9, 2017 and last used on April 12, 2022, the day of the attack.

53. According to records from Lyft, the AOL Account is connected to FRANK JAMES's Lyft account, which he used in the week before the attack to travel to and from his apartment and his storage unit in preparation of the attack. Thus, the AOL Account will likely contain records related to the defendant's Lyft trips. According to records from PayPal, in addition to the Microsoft Account, the AOL Account was also connected to JAMES's PayPal account which he used to purchase smoke grenades. Thus, the AOL Account will likely contain records related to JAMES's purchase of the smoke grenades. Accordingly, there is probable

cause that the AOL Account will contain evidence of the Subject Offenses, including evidence of JAMES's planning of the attack and his identity as the individual carrying out the attack.

iv. The Mail.com Account

54. There is probable cause to search the Mail.com Account. According to records from 1&1, the subscriber of the Mail.com Account is "Frank James." The Mail.com Account was created on or about December 10, 2011, and last accessed on April 11, 2022. In addition, the Mail.com Account was logged into the James Samsung Phone.

55. FRANK JAMES used the Mail.com Account in connection with preparing and planning of the attack. For example, according to records from Fireworks Company-1 on or about June 21, 2021, JAMES provided this Mail.com Account email address to Fireworks Company-1 when purchasing the same brand of fireworks found at the scene of the attack. On or about January 20, 2022, JAMES listed his Mail.com Account when making a reservation with a management company for the short-term rental apartment in Philadelphia that JAMES stayed in before committing the attack. JAMES communicated via email using his Mail.com Account with the rental company on or about March 27, 2022. According to records from 1&1, JAMES also used his Mail.com Account in connection with renting storage unit #0318 and renting the U-Haul that he drove to the attack on April 12, 2022. Accordingly, there is probable cause that the Mail.com Account will contain evidence of the Subject Offenses, including evidence of JAMES's planning of the attack and his identity as the individual carrying out the attack.

v. The Facebook Account

56. There is probable cause to search the Facebook Account. According to records from Facebook, the subscriber of the Facebook Account is listed as "Frank Whitaker," one of FRANK JAMES's pseudonyms, with the subscriber email address of

frankjames20048@msn.com, the Microsoft Account. The payment information associated with the Facebook Account is JAMES's credit card number. The account was registered on or about September 8, 2009.

57. FRANK JAMES used the Facebook Account to post YouTube videos in which he discussed future violence as well as other images, such as someone pointing a gun at the camera four days before his attack, indicating JAMES's intent to commit an attack. JAMES also posted other photographs on his Facebook Account which will identify him as the individual in the YouTube videos. Accordingly, there is probably cause that the Facebook Account will contain evidence of the Subject Offenses, including JAMES's motive, his planning of the attack, and his identity as the individual posting the YouTube videos and carrying out the attack.

vi. The Apple Account

58. There is probable cause to search the Apple Account. According to records from Apple, the subscriber of the Apple account is Frank James. The subscriber email address of the Apple Account is listed as the Microsoft Account's email address. The account was created on or about March 1, 2016 and the data was last backed up on or about April 12, 2022. Records from Apple indicate that there is an iCloud account associated with the Apple Account and that the iCloud backup feature is enabled for bookmarks, calendars, and iCloud Drive.

59. In addition, based on the review of the Apple records, the "iForgot" function of the Apple Account was used twice on or about April 12, 2022, the day of the attack, to attempt to log into the Apple Account. Accordingly, there is probable cause that the Apple Account will contain evidence of the Subject Offenses, including JAMES's motive, his planning of the attack, his location when planning and carrying out the attack.

BACKGROUND ON GOOGLE

60. In my training and experience, I have learned that Google is a company that provides a variety of services that can be accessed from traditional computers and other electronic devices running various operating systems via web browsers or mobile and desktop applications created by Google ("apps"). As described in further detail below, the services include email, file storage and management, voice over internet calling, electronic messaging, and Internet search.

61. *Gmail.* In my training and experience, I know that Google allows subscribers to obtain email accounts at the domains gmail.com and googlemail.com. Subscribers obtain an account by registering with Google, and store, send, and receive email by accessing Google's servers. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users and the communications themselves may discuss crimes or reflect a conspiracy to do so. Similarly, users can send and receive emails with attached documents and other types of files, such as audio recordings, video files, and photographs, to their emails which may themselves constitute evidence of the crimes under investigation.

62. *Google Calendar and Contacts.* Google account holders can also maintain address books, contact or buddy lists and calendar data on servers maintained and/or owned by Google. In my training and experience, evidence of who was using a Google account may be

found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files. Calendar and contact information can also assist investigators to identify coconspirators, and provide contextual information necessary to understand other evidence obtained in the investigation, for example, the significance of a presentation slide deck shown at a meeting documented in a calendar event, and a subsequent email confirming an understanding reached at the meeting.

63. *Google Voice*. In my training and experience, Google also provides its users with the ability to make and receive audio calls and to send and receive text messages over the Internet directly to traditional telephones. Google calls its service "Google Voice" and allows its users to obtain a free telephone number associated with their Google Voice account that will allow them to receive calls, text messages, and voicemail messages through Google Voice. Indeed, Google Voice is capable of transcribing a user's voicemail messages and rendering them text searchable. Audio and video calls can be made using Google Voice from a user's computer or smartphone as long as the user is connected to the Internet. Thus, Google retains records of such calls, but a user's telephone service provider does not retain call history reflecting Google Voice calls. To offer these services, Google Voice saves and processes its users' call, text, and voicemail information.

64. *Google Plus*. Google also operates a free-access social networking website called Google+, located at www.plus.google.com. Google+ allows Google account holders to share written news, photographs, videos, and other information with other Google+ users who following the user, or with "collections" or "communities" followed by Google+ users. Google+ users can also post comments in response and choose to share them with other users.

65. *Google Hangouts*. Google Hangouts is a unified communications service that allows Google account holders to initiate and participate in text, voice or video chats, either one-on-one or in a group. Hangouts is a communication service built into Google+ and Gmail. Google Hangouts can also integrate with Google Voice, allowing users of that service to make free domestic phone calls from their electronic devices. Google offers Hangouts mobile apps for download that can be used on electronic devices running Apple's iOS or Google's Android operating systems.

66. *Google Drive and Google Photos*. Google provides a cloud storage service called "Google Drive" that permits Google account holders to store up to 15 gigabytes of data on Google's servers for free, and more for an additional charge. Google users can share and download that data, including images, audio files, video files, word processing documents, spreadsheets, presentation files, and PDFs from their electronic devices through the Google Drive application, or by logging into their Google account using a web browser on any electronic device. The Google Drive application, which runs on both desktop and mobile devices, allows Google users to automatically back up files on their electronic devices to their Google Drive and sync them, so that changes to documents saved on the device are automatically saved on Google Drive and accessible from the user's other devices. As part of Google Drive, Google allows its users to create and collaboratively edit documents with other users using Google Docs (word processing), Google Sheets (spreadsheets), Google Slides (presentations), and Google Forms (fillable forms). Similarly, photographs saved in a Google user's Drive are then accessible to the user through the "Google Photos" service. Google separately provides a Google Photos application for electronic devices that, similar to the Google Drive application, allows users to share, edit, and automatically back up their photographs from their electronic devices.

67. *Google Translate*. Google offers users a web-based and application based translation service that will translate text from one language to another. The application can also be used to translate web pages, audio recordings, and text appearing in photos.

68. *Web & App Activity.* Google collects and retains a wide variety of data on its account holders' use of Google applications and services. The data collected and retained by Google includes the following:

a. *Location History.* Google collects data on the location of their users from their electronic devices. Google uses this information for, among other things, location-based advertising, location-based search results, embedding location information in the photographs and videos taken by the user (known as geo-tagging), navigation through the "Google Maps" service and related applications, and features that permit users to locate their mobile electronic devices if they lose them.

b. *Browser and Search History.* Google operates a popular Internet search engine, browser software that runs on both traditional computers and on mobile electronic devices, and an operating system for mobile electronic devices. Google retains browser and search history when a user views a web page or conducts an Internet search while logged into their Google account, or when they use Google's "Chrome" web browser or another Google desktop or mobile app to browse or search the Internet. Google account holders can also choose to synchronize Chrome data, including bookmarks, browser and search history, passwords, and other settings across multiple electronic devices when the user is signed into Chrome on each device. By default, when a user signs in to Chrome, all the

user's Chrome data will be synced to the user's Google account by saving that data on Google's servers.

69. *Google My Maps.* Google provides a service that enables users to create custom maps for personal use or sharing called "Google My Maps." Google My Maps allows users to add points, lines and shapes on top of Google Maps, using an editing program.

70. *Google Play*. Google operates a digital distribution service for mobile electronic devices running the Android operating system called "Google Play." Google Play allows users to browse and download applications developed with the Android software development kit and published through Google. Google collects and retains information about its account holders' searches in Google Play and the applications that they are downloading to their devices. Google also uses Google Play to sync information on mobile devices running Google's Android operating system with the user's Google Account.

71. In my training and experience, evidence of who was using a Google account and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

72. The stored communications and files connected to a Google account may provide direct evidence of the offenses under investigation. I know that instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. In addition, the user's account activity, logs, stored electronic communications, and other data retained by

Google can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Additionally, stored electronic data may provide more precise information about the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email or saved to cloud storage). Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

73. Finally, stored electronic data frequently provides relevant insight into the account owner's state of mind as it relates to the offense under investigation. For example, information in the account may indicate the owner's motive and intent to commit a crime including communications, browser and search history relating to preparation to commit crimes, or consciousness of guilt, such as deleting communications or other inculpatory data in an effort to conceal them from law enforcement. Photographs and videos can provide visual evidence of a coconspirator's participation in a critical meeting and help to identify other participants in the conspiracy who were previously unknown to law enforcement.

74. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account

may indicate the owner's motive and intent to commit a crime (e.g., browser history indicating planning or preparation to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement). Other information connected to a Google account may lead to the discovery of additional evidence. A list of apps might reveal banking institutions and online trading accounts used by the subjects, or the identification of other means and methods of communication. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation. Therefore, Google's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Google's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users and other participants in the criminal conduct under investigation.

BACKGROUND ON MICROSOFT

75. In my training and experience, I have learned that Microsoft provides a variety of online services to the public, including email, cloud storage (offered under the OneDrive and SharePoint brands) and real-time chat services (offered under the Skype brand). The computers of Microsoft are likely to contain stored electronic communications (including retrieved and unretrieved email and Skype chats); files stored by subscribers in their cloud storage accounts; and information concerning subscribers and their use of Microsoft services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

76. In general, an email that is sent to a Microsoft subscriber is stored in the subscriber's "mail box" on the provider's servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Microsoft's servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Microsoft's servers for a certain period of time. Similarly, chats that a subscriber sends or receives can remain in storage on the provider's servers indefinitely.

77. A Microsoft subscriber can also store with the provider files in addition to emails and chats, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), videos, documents and other files, on servers maintained and/or owned by Microsoft. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files. These additional files may themselves contain evidence of the crimes under investigation in addition to evidence relating to the identities of those involved in the crimes.

78. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, this information can provide clues to their identity, location or illicit activities.

79. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the IP address used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

80. In my training and experience, in some cases, email account users communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

81. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled

the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the IP addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

BACKGROUND ON FACEBOOK

82. Facebook is a service owned by Meta Platforms, a United States company and a provider of an electronic communications service as defined by 18 U.S.C. §§ 3127(1) and 2510. Specifically, Facebook is a free-access social networking service, accessible through its website and mobile application, that allow subscribers to acquire and use Facebook accounts through

which users can share messages, multimedia, and other information with other Instagram users and the general public.

83. Facebook collects basic contact and personal identifying information from users during the Instagram registration process. This information, which can later be changed by the user, may include the user's full name, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, credit card or bank account number, and other personal identifiers. Facebook keeps records of changes made to this information.

84. Facebook also collects and retains information about how each user accesses and uses Instagram. This includes information about the Internet Protocol ("IP") addresses used to create and use an account, unique identifiers and other information about devices and web browsers used to access an account, and session times and durations.

85. Each Facebook account is identified by a unique username chosen by the user. Users can change their usernames whenever they choose but no two users can have the same usernames at the same time. Facebook users can create multiple accounts and, if "added" to the primary account, can switch between the associated accounts on a device without having to repeatedly log-in and log-out.

86. Facebook users can also connect their Facebook accounts to utilize certain cross-platform features. Facebook accounts can also be connected to certain third-party websites and mobile apps for similar functionality. Facebook maintains records of changed Instagram and Facebook usernames, associated Instagram and Facebook accounts, and previous and current connections with accounts on Facebook and third-party websites and mobile apps.

87. Facebook users can "follow" other users to receive updates about their posts and to gain access that might otherwise be restricted by privacy settings (for example, users can choose whether their posts are visible to anyone or only to their followers). Users can also "block" other users from viewing their posts and searching for their account, "mute" users to avoid seeing their posts, and "restrict" users to hide certain activity and prescreen their comments.

88. Users have several ways to search for friends and associates to follow on Facebook, such as by allowing Facebook to access the contact lists on their devices to identify which contacts Facebook users. Facebook retains this contact data unless deleted by the user and periodically syncs with the user's devices to capture changes and additions. Users can similarly allow Facebook to search an associated Facebook account for friends who are also Instagram users. Users can also manually search for friends or associates.

89. Each Facebook user has a profile page where certain content they create and share ("posts") can be viewed either by the general public or only the user's followers, depending on privacy settings. Users can customize their profile by adding their name, a photo, a short biography ("Bio"), and a website address.

90. Users can interact with posts by liking them, adding or replying to comments, or sharing them within or outside of Facebook. Users receive notification when they are tagged in a post by its creator or mentioned in a comment (users can "mention" others by adding their username to a comment followed by "@"). Users may also send direct messages over the platform.

91. Facebook also offers services called Facebook Pay for users to make purchases, donate money, and conduct other financial transactions on Facebook and other associated

websites and apps. Facebook collects and retains payment information, billing records, and transactional and other information when these services are utilized.

92. Facebook also has a search function which allows users to search for accounts by username, user activity by location, and user activity by hashtag. Hashtags, which are topical words or phrases preceded by a hash sign (#), can be added to posts to make them more easily searchable and can be "followed" to generate related updates from Instagram. Facebook retains records of a user's search history and followed hashtags.

93. Facebook collects and retains location information relating to the use of an Instagram or Facebook account, including user-entered location tags and location information used by Facebook to personalize and target advertisements.

94. Facebook uses information it gathers from its platforms and other sources about the demographics, interests, actions, and connections of its users to select and personalize ads, offers, and other sponsored content. Facebook maintains related records for Instagram and Facebook users, including information about their perceived ad topic preferences, interactions with ads, and advertising identifiers. This data can provide insights into a user's identity and activities, and it can also reveal potential sources of additional evidence.

95. In some cases, Facebook users may communicate directly with Facebook about issues relating to their accounts, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

96. For each Facebook user, Facebook collects and retains the content and other records described above, sometimes even after it is changed by the user (including usernames, phone numbers, email addresses, full names, privacy settings, email addresses, and profile bios and links).

97. In my training and experience, evidence of who was using Instagram and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

98. For example, the stored communications and files connected to an account may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

99. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Facebook can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device

identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

100. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

101. Other information connected to the use of Facebook may lead to the discovery of additional evidence. For example, lists of the account owner's friends, private messages, may reveal other groups and money laundering services used in furtherance of the Subject Offenses or other communications services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

102. Therefore, Facebook's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Facebook. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

BACKGROUND ON APPLE[5]

103. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

104. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct audio and video calls.

c. iCloud is a cloud storage and cloud computing service from Apple that allows its users to interact with Apple's servers to utilize iCloud-connected services to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-

---

[5] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at https://www.apple.com/legal/privacy/law-enforcement-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on iCloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iCloud Backup allows users to create a backup of their device data. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

d. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

e. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

f. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

g. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or

Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

105. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. The account identifier for an Apple ID is an email address, provided by the user. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

106. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to

and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

107. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

108. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs into FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including

communications regarding a particular Apple device or service, and the repair history for a device.

109. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

110. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

111. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation by showing the defendant's planning and motive for committing the attack. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

112. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

113. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

114. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and

iTunes Store may reveal services used in furtherance of the crimes under investigation. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of possible co-conspirators and instrumentalities of the crimes under investigation.

115. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

BACKGROUND CONCERNING EMAIL

116. In my training and experience, I have learned that Yahoo Inc. (AOL) and 1&1 (together the "Providers") provide a variety of on-line services, including electronic mail ("email") access, to the public. Each of the Providers allows subscribers to obtain email accounts at a domain name associated with the Provider. Subscribers obtain an account by registering with the Providers. During the registration process, the Providers ask subscribers to provide basic personal information. Therefore, the computers of the Providers are likely to contain stored electronic communications (including retrieved and unretrieved email for the Providers' subscribers) and information concerning subscribers and their use of the Providers' services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

117. A subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails),

and other files, on servers maintained and/or owned by the Providers. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

118. In addition, I am aware that the Providers offer a service through which a computer user can search webpages for text that the user types in, and that under some circumstances the Providers save the user's text searches for later retrieval. I am also aware that the Providers may also keep records of the webpages or IP addresses that a user clicks on or types directly into his web browser's address bar, if the user is logged into his/her account at the time.

119. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users. Based on my training and my experience, I know that even if subscribers insert false information to conceal their identity, I know that this information often provide clues to their identity, location or illicit activities.

120. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage

of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

121. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

122. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed

or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculpate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (e.g., location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (e.g., communications relating to the crime), or consciousness of guilt (e.g., deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

123. Based on the forgoing, I request that the Court issue the proposed search warrant.

124. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on the providers listed above. Because the warrant will be served on the providers, who will then compile the requested records at a time convenient to them, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,

Ian Franckling
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone on _____, 2022

Ramon E. Reyes, Jr. Digitally signed by Ramon E. Reyes, Jr. Date: 2022.11.01 10:48:58 -04'00'

HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A1

Property to Be Searched

This warrant applies to information associated with the following accounts:

Account	User
profitofdoom8888@gmail.com	FRANK JAMES
Prophetoftruth88@gmail.com	FRANK JAMES

(the "Google Accounts") that are stored at premises controlled by Google LLC ("Google"), an electronic communication and remote computing service provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B1

Particular Things to be Seized

I. Information to be disclosed by Google LLC

To the extent that the information described in Attachment A1 is within the possession, custody, or control of Google, regardless of whether such information is located within or outside of the United States, including any emails, records, files, logs, or information that has been deleted but is still available to Google, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Google is required to disclose the following information to the government for the Account or identifiers listed in Attachment A1 (the "Account"), from January 1, 2017 to the present:

a. All records or other information regarding the identification of the Account and the users of the Account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

b. All account change history;

c. All records or other information regarding the devices associated with, or used in connection with, the Account, including cookies, push tokens, serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile

Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

d. All device logs for the Account;

e. All subscriber and non-content communication records pertaining to any other account linked to the identified Account by a secondary or recovery email address or telephone number, or by cookies, push tokens, serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

f. The contents of all emails associated with the Account, including stored or preserved copies of emails sent to and from the Account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

g. The contents of all text and voice messages ("messages") associated with the Account (including voicemails, SMS messages, and MMS messages), including stored or

preserved copies of messages sent to and from the Account (including all draft and deleted messages), the source and destination account or phone number associated with each message, the date and time at which each message was sent and received, the size and length of each message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each message;

h. All Google service data and content associated with the Account, including data and content associated with: Gmail, Google Hangouts, YouTube, Android, Location History, Google Calendar, Google Keep, Chromeos Login, and any other services associated with the Account. The Google service data and content associated with the Account include, without limitation: emails, voicemails, text messages, address books, contact and buddy lists, notes, reminders, calendar entries, image files, video files, audio files, word processing documents, spreadsheets, presentations, PDFs, bookmarks, and device settings;

i. All browsing history and search history associated with the Account, including: Chrome browsing history, Google Search queries and history, Google Maps queries and history, Google Translate queries and history (including original text, photographs, audio files, and web page URLs submitted for translation, and the translation provided in response to such queries), and search history associated with any third-party search application or search engine;

j. All location data associated with the Account, including Global Positioning System ("GPS") data, cell site/cell tower triangulation/trilateration, and precision measurement information such as timing advance or per call measurement data, and Wi-Fi location, including the GPS coordinates and the dates and times of all location recordings;

k. All device backups associated with the Account;

l. All Google application data and third-party application data associated with the Account;

m. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including Google activity logs, Gmail logs, Google Voice logs, Google Hangouts logs, Google Developers Console logs, Google Drive logs, Google Play logs (including purchases, downloads, and updates of Google and third-party apps), messaging logs (including Google Hangouts, Google Voice, Google Profile, Google+, SMS, and MMS messages), password recovery logs, sign-on logs for all Google services, logs associated with device activation and upgrades, and logs associated with web-based access of Google services (including all cookies, IP addresses, browser information, and device identifiers associated with such access);

n. All other data and records, including content, relating to the services used by the Account;

o. All records pertaining to communications between Google and any person regarding the Account, including contacts with support services and records of actions taken; and

p. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Google.

Google is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of 18 U.S.C. § 1992(a)(7) and (b)(1) (terrorist attacks or other violence against mass transportation systems) and § 924(c)(iii) (use of a firearm during a crime of violence) (the "Subject Offenses") those violations involving Frank James and occurring after January 1, 2017 including, for each account or identifier listed on Attachment A1, information pertaining to the following matters:

(a) The motive, planning, and execution of an attack;

(b) The use of a firearm;

(c) The purchasing of firearms, ammunition, smoke emitting devices, fireworks, and any other weapon;

(d) Records and any other communications related to purchases of cellular telephones;

(e) Videos, emails, communications, records, reflecting a motive or planning of an attack;

(f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(i) The identity of the person(s) who communicated with the user ID about matters relating to the Subject Offenses, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT A2

Property to Be Searched

This warrant applies to information associated with the following accounts:

Account	User
frankjames20048@msn.com	FRANK JAMES

(the "Microsoft Account") that is stored at premises controlled by Microsoft Corp. ("Microsoft"), an electronic communication and remote computing service provider headquartered at One Microsoft Way, Redmond, Washington.

ATTACHMENT B2

Particular Things to be Seized

I. Information to be disclosed by Microsoft Corp.

To the extent that the information described in Attachment A2 is within the possession, custody or control of Microsoft (or the "Provider"), regardless of whether such information is located within or outside of the United States, and including any emails, chats records, files, logs or information that has been deleted but is still available to Microsoft, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Microsoft is required to disclose the following information to the government for each account or identifier listed in Attachment A2 from January 1, 2017 to the present:

a. The contents of all emails associated with the Microsoft Account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent and the size and length of each email:

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, login IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

c. The types of service utilized;

d. Information regarding the device used to send and receive email or conduct chats;

e. All records or other information stored by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, files, and cloud-stored data;

f. Information regarding the location of the account user; and

g. All records pertaining to communications between each Provider and any person regarding the account, including contacts with support services and records of actions taken.

Microsoft is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of 18 U.S.C. § 1992(a)(7) and (b)(1) (terrorist attacks or other violence against mass transportation systems) and § 924(c)(iii) (use of a firearm during a crime of violence) (the "Subject Offenses") those violations involving Frank James and occurring after January 1, 2017 including, for each account or identifier listed on Attachment A2, information pertaining to the following matters:

(a) The motive, planning, and execution of an attack;

(b) The use of a firearm;

(c) The purchasing of firearms, ammunition, smoke emitting devices, fireworks, and any other weapon;

(d) Records and any other communications related to purchases of cellular telephones;

(e) Videos, emails, communications, records, reflecting a motive or planning of an attack;

(f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(i) The identity of the person(s) who communicated with the user ID about matters relating to the Subject Offenses, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT A3

Property to Be Searched

This warrant applies to information associated with the following accounts:

Account	User
frankjames20048@aol.com	FRANK JAMES

(the "AOL Account") that is stored at premises controlled by Yahoo Inc. (formerly known as Oath Holdings Inc. and AOL) ("AOL"), an electronic communication and remote computing service provider that accepts service of legal process at 1199 Coleman Avenue, San Jose, CA 95110.

ATTACHMENT B3

Particular Things to be Seized

III. Information to be disclosed by Yahoo Inc. (AOL)

To the extent that the information described in Attachment A3 is within the possession, custody, or control of Yahoo Inc. (or the "Provider"), including any emails, records, files, logs, or information that has been deleted but is still available to Yahoo Inc., or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Yahoo Inc. is required to disclose the following information to the government for each account or identifier listed in Attachment A3 from January 1, 2017 to the present:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. The text of all Internet search requests input by the subscriber; and all URLs or IP addresses typed into the address bar or URLs or IP addresses clicked on;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of service utilized;

e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

g. All accounts accessed by the browser(s) and device(s) associated with the account listed above, as determined by an analysis of cookies and/or machine cookies.

Yahoo, Inc. (AOL) is hereby ordered to disclose the above information to the government within fourteen of issuance of this warrant.

IV. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of 18 U.S.C. § 1992(a)(7) and (b)(1) (terrorist attacks or other violence against mass transportation systems) and § 924(c)(iii) (use of a firearm during a crime of violence) (the "Subject Offenses") those violations involving Frank James and occurring after January 1, 2017 including, for each account or identifier listed on Attachment A3, information pertaining to the following matters:

(a) The motive, planning, and execution of an attack;

(b) The use of a firearm;

(c) The purchasing of firearms, ammunition, smoke emitting devices, fireworks, and any other weapon;

(d) Records and any other communications related to purchases of cellular telephones;

(e) Videos, emails, communications, records, reflecting a motive or planning of an attack;

(f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(i) The identity of the person(s) who communicated with the user ID about matters relating to the Subject Offenses, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT A4

Property to Be Searched

This warrant applies to information associated with the following accounts:

Account	User
frankjames1326@mail.com	FRANK JAMES

(the "Mail.com Account") that is stored at premises controlled by 1&1 IONOS Inc. ("Mail.com"), an electronic communication and remote computing service provider that accepts service of legal process at 701 Lee Road, Suite 300, Chesterbrook, PA 19087.

ATTACHMENT B4

Particular Things to be Seized

I. Information to be disclosed by 1&1 (mail.com)

To the extent that the information described in Attachment A4 is within the possession, custody, or control of 1&1 ("Mail.com") (or the "Provider"), including any emails, records, files, logs, or information that has been deleted but is still available to Mail.com, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Mail.com is required to disclose the following information to the government for each account or identifier listed in Attachment A4 from January 1, 2017 to the present:

a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;

b. The text of all Internet search requests input by the subscriber; and all URLs or IP addresses typed into the address bar or URLs or IP addresses clicked on;

c. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);

d. The types of service utilized;

e. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

f. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken;

g. All accounts accessed by the browser(s) and device(s) associated with the account listed above, as determined by an analysis of cookies and/or machine cookies.

1&1(mail.com) is hereby ordered to disclose the above information to the government within fourteen of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of 18 U.S.C. § 1992(a)(7) and (b)(1) (terrorist attacks or other violence against mass transportation systems) and § 924(c)(iii) (use of a firearm during a crime of violence) (the "Subject Offenses") those violations involving Frank James and occurring after January 1, 2017 including, for each account or identifier listed on Attachment A4, information pertaining to the following matters:

(j) The motive, planning, and execution of an attack;

(k) The use of a firearm;

(l) The purchasing of firearms, ammunition, smoke emitting devices, fireworks, and any other weapon;

(m) Records and any other communications related to purchases of cellular telephones;

(n) Videos, emails, communications, records, reflecting a motive or planning of an attack;

(o) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(p) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(q) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(r) The identity of the person(s) who communicated with the user ID about matters relating to the Subject Offenses, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT A5

Property to Be Searched

This warrant applies to information associated with the following accounts:

Account Number	Display Name	User
10000258632238	Frank Whitaker	FRANK JAMES

(the "Facebook Account") that is stored at premises owned, maintained, controlled, or operated by Meta Platforms Inc. ("Meta"), an electronic communication and remote computing service provider headquartered at 1601 Willow Road in Menlo Park, California.

ATTACHMENT B5

Particular Things to be Seized

I. Information to be disclosed by Meta, Inc. (Facebook)

To the extent that the information described in Attachment A5 is within the possession, custody, or control of Meta Inc. ("Facebook"), regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Facebook, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Facebook is required to disclose the following information to the government for the user ID listed in Attachment A5 from January 1, 2017 to the present:

(a) All contact and personal identifying information, including**:** full name, user identification number, birth date, gender, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.

(b) All activity logs for the account and all other documents showing the user's posts and other Facebook activities;

(c) All photos and videos uploaded by that user ID and all photos and videos uploaded by any user that have that user tagged in, including Exchangeable Image File ("EXIF") data and any other metadata associated with those photos and videos;

(d) All profile information; News Feed information; status updates; videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which

the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;

(e) All records or other information regarding the devices and internet browsers associated with, or used in connection with, that user ID, including the hardware model, operating system version, unique device identifiers, mobile network information, and user agent string;

(f) All other records and contents of communications and messages made or received by the user, including all Messenger activity, private messages, chat history, video and voice calling history, and pending "Friend" requests;

(g) All "check ins" and other location information;

(h) All IP logs, including all records of the IP addresses that logged into the account;

(i) All records of the account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

(j) All information about the Facebook pages that the account is or was a "fan" of;

(k) All past and present lists of friends created by the account;

(l) All records of Facebook searches performed by the account;

(m) All information about the user's access and use of Facebook Marketplace;

(n) The types of service utilized by the user;

(o) The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);

(p) All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;

(q) All records pertaining to communications between Facebook and any person regarding the user or the user's Facebook account, including contacts with support services and records of actions taken.

Meta Inc. is hereby ordered to disclose the above information to the government within fourteen of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of 18 U.S.C. § 1992(a)(7) and (b)(1) (terrorist attacks or other violence against mass transportation systems) and § 924(c)(iii) (use of a firearm during a crime of violence) (the "Subject Offenses") those violations involving Frank James and occurring after January 1, 2017 including, for each account or identifier listed on Attachment A5, information pertaining to the following matters:

(a) The motive, planning, and execution of an attack;

(b) The use of a firearm;

(c) The purchasing of firearms, ammunition, smoke emitting devices, fireworks, and any other weapon;

(d) Records and any other communications related to purchases of cellular telephones;

(e) Videos, emails, communications, records, reflecting a motive or planning of an attack;

(f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(i) The identity of the person(s) who communicated with the user ID about matters relating to the Subject Offenses, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

ATTACHMENT A6

Property to Be Searched

This warrant applies to information associated with the following accounts:

Account	User
frankjames20048@msn.com	FRANK JAMES

(the "Apple Account") that is stored at premises owned, maintained, controlled, or operated by Apple Inc. ("Apple"), an electronic communications service and/or remote computing service provider headquartered at One Apple Park Way, Cupertino, California.

ATTACHMENT B6

Particular Things to be Seized

I. Information to be disclosed by Apple Inc. ("Apple")

To the extent that the information described in Attachment A6 is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to Apple, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government for each account or identifier listed in Attachment A6 from January 1, 2017 to the present:

h. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

i. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers

("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and International Mobile Station Equipment Identities ("IMEI");

j. The contents of all emails associated with the account January 1, 2017 to present, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

k. The contents of all instant messages associated with the account January 1, 2017 to present including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

l. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

m. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging

and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

n. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

o. All records pertaining to the types of service used;

p. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

q. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within fourteen of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and instrumentalities of 18 U.S.C. § 1992(a)(7) and (b)(1) (terrorist attacks or other violence against mass transportation systems) and § 924(c)(iii) (use of a firearm during a crime of violence) (the "Subject Offenses") those violations involving Frank James and occurring after January 1, 2017 including, for each account or identifier listed on Attachment A6, information pertaining to the following matters:

(a) The motive, planning, and execution of an attack;

(b) The use of a firearm;

(c) The purchasing of firearms, ammunition, smoke emitting devices, fireworks, and any other weapon;

(d) Records and any other communications related to purchases of cellular telephones;

(e) Videos, emails, communications, records, reflecting a motive or planning of an attack;

(f) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;

(g) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;

(h) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

(i) The identity of the person(s) who communicated with the user ID about matters relating to the Subject Offenses, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.